# Avaliação do Desempenho de Sistemas de Segurança com Suporte de WPA

Luís Barreto[1] e Susana Sargento[2]
[1]Instituto Politécnico de Viana do Castelo, Escola Superior de Ciências Empresariais, Valença, Portugal
Phone: +351 251800840, Fax: +351 251800841, e-mail: lbarreto@esce.ipvc.pt
[2]Universidade de Aveiro, Instituto de Telecomunicações, Aveiro, Portugal
Phone: +351 234377900, Fax: +351 234377901, e-mail: ssargento@det.ua.pt

***Resumo* - Actualmente, a segurança em redes sem fios é uma das áreas de investigação que representa grandes desafios. Para ser possível garantir a segurança neste tipo de redes a *Wi-Fi Alliance* definiu o protocolo WPA. Este é um protocolo que, utilizando equipamentos actuais, tem como objectivo garantir de forma eficaz e robusta a segurança numa rede sem fios. Este artigo apresenta um estudo experimental da solução de segurança WPA, tendo em conta aspectos de desempenho de segurança, e custos de desempenho introduzidos na rede e nos seus equipamentos. Os resultados observados mostram que o WPA, na sua versão EAP-TLS, é resistente a ataques do tipo *homem no meio*, personificação e controlo de sessão. Ao nível do desempenho da rede e dos seus equipamentos, este não diminui de forma significativa com a utilização do WPA.**

## I. INTRODUÇÃO

A crescente utilização das redes sem fios como meio de transporte de informação tem aumentado de forma significativa a necessidade de se utilizarem mecanismos de segurança para proteger a informação transmitida e os seus intervenientes. A primeira tentativa do IEEE de introduzir um mecanismo de segurança nas redes sem fios deu origem ao *Wired Equivalent Protocol* (WEP) [1]. Este mecanismo cedo se mostrou incapaz, apresentando inúmeras falhas, e sendo alvo de inúmeros ataques, o que levou o IEEE a criar o grupo de trabalho *i*. Este grupo tem como objectivo definir um conjunto de mecanismos que realmente garantam a protecção e a segurança das redes sem fios. O resultado final do seu trabalho será a norma IEEE 802.11*i* [4]. No entanto, como os resultados do seu trabalho não estariam concluídos num espaço de tempo curto, a *Wireless-Fidelity (Wi-Fi) Alliance* [2] definiu um mecanismo possível de ser implementado imediatamente, robusto e eficiente: o *Wi-Fi Protected Access* (WPA) [3].

O WPA é baseado no 802.11*i* sendo, ao contrário do 802.11*i*, compatível com equipamentos WEP actuais, através de uma actualização de *firmware* dos *Access Points* (APs) e placas de rede. O WPA garante a segurança em redes *Wi-Fi* com a introdução de um algoritmo de cifra robusto, bem como a introdução de autenticação por utilizador. Na descrição do protocolo refere-se a garantia de que os dados de cada utilizador permanecem protegidos, e que apenas utilizadores autorizados podem aceder aos recursos da rede. Outro dos objectivos do WPA é também a autenticação mútua entre o cliente e o AP.

Atendendo às capacidades e às características do WPA, é importante conhecer qual o nível de segurança e de eficiência assegurado pelo WPA, assim como o custo ao nível da rede e dos equipamentos introduzido pela sua utilização. Este artigo apresenta um estudo sobre os serviços que constituem o WPA. São também apresentados um conjunto de testes que permitem avaliar o WPA ao nível da segurança e dos custos de desempenho introduzidos na rede e nos equipamentos.

O artigo encontra-se organizado da seguinte forma. A secção II apresenta um estudo sobre os mecanismos que constituem o WPA. A experimentação e os resultados obtidos são apresentados na secção III. As conclusões são apresentadas na secção IV.

## II. WPA

O WPA é compatível e pode ser utilizado como solução de segurança em todas as variantes IEEE 802.11, incluindo 802.11*a*, *b* e *g*.

Para melhorar a codificação dos dados, o WPA utiliza o *Temporal Key Integrity Protocol* (TKIP) [4] que fornece melhorias consideráveis ao nível da cifra dos dados com chaves temporárias. O WPA inclui ainda uma função de mistura de chaves por pacote de dados, uma mensagem para verificação da integridade dos dados *Message Integrity Check* (MIC), vectores de inicialização (*Initialization Vectors* - IV) estendidos com regras de sequenciação, e um mecanismo de renovação de chaves. Ao contrário do mecanismo de verificação da integridade da mensagem WEP, o MIC é obtido recorrendo a um método não linear, o que garante a protecção de integridade das mensagens. O WPA utiliza IV de 48 *bits* para eliminar muitos dos defeitos apontados aos IVs utilizados no WEP. Na secção *A* são apresentados com mais detalhe o TKIP e cada um dos seus componentes.

Outra das falhas apontadas ao WEP é o facto de este não incluir um mecanismo de controlo de acesso à rede. O WPA utiliza como mecanismo de controlo de acesso o protocolo 802.1X [1]. Este mecanismo garante a autenticação dos utilizadores e permite derivar chaves de sessão que depois são utilizadas para derivar as chaves temporárias. A secção *B* apresenta uma pequena descrição deste mecanismo.

*A TKIP*

O TKIP [4] elimina, utilizando *hardware* já existente e mantendo o protocolo criptográfico *Rivest Code* 4 (RC4) [6] utilizado no WEP, algumas das suas falhas. O TKIP aumenta o tamanho da chave de cifra de 40 para 128 *bits* e substitui a chave única e estática do WEP por chaves que são geradas dinamicamente e distribuídas pelo servidor de autenticação. O TKIP utiliza uma metodologia de hierarquias e de gestão de chaves que elimina a previsibilidade das mesmas.

As principais orientações que levaram ao desenvolvimento do TKIP são as seguintes: (1) não re-utilização do mesmo vector de inicialização (IV) com a mesma chave de sessão – dois pacotes diferentes nunca deverão ser cifrados com a mesma chave, de modo a garantir protecção contra ataques de colisão (re-utilização de chaves); (2) utilização de um número de sequência e rejeição dos pacotes que são recebidos fora de ordem, garantindo-se assim protecção contra ataques de repetição; (3) geração automática de chaves aleatórias – a chave de sessão deve ser gerada antes de iniciado o contador de IV; (4) geração de chaves por pacote – de modo a evitar geração de chaves fracas, as chaves de sessão são processadas por um esquema de mistura de chaves, que depois são utilizadas pelo gerador RC4; (5) nova função de integridade da mensagem – é utilizada uma função de *hash* criptograficamente segura em substituição do valor linear *Cyclic Redundancy Check* (CRC) utilizado no WEP. O CRC obtido de forma linear no WEP denomina-se de *Integrity Check Value* (ICV).

Como já foi referido, os mecanismos que implementam o TKIP são o MIC, sequenciação IV/extensão do IV e geração de chaves por pacote/distribuição de chaves. De seguida, apresentam-se esses mecanismos.

*A.1. MIC*

O mecanismo de verificação da integridade das mensagens no WEP é obtido por um algoritmo linear e é apenas função dos dados a enviar. Para resolver esse problema, o TKIP utiliza uma função de *hash* segura, denominado de MIC. O MIC utiliza uma chave denominada chave MIC. Esta chave é diferente nos dois sentidos da comunicação, e é computacionalmente independente das chaves criptográficas utilizadas. O MIC destina-se a prevenir que um intruso obtenha pacotes de dados, os altere e volte a reenviá-los. Para isso, fornece uma função matemática pela qual o receptor e o emissor efectuam o cálculo e comparação da chave MIC: se o resultado das funções no emissor e receptor for diferente, assume-se que os dados foram violados e o pacote é eliminado.

A Figura 1 representa o processo de geração do MIC que, tal como indica a figura, depende de um algoritmo que é função do endereço MAC de destino, do endereço MAC de origem, da informação a enviar e da chave MIC. O algoritmo gera um código de *hash* com 64 *bits* (8 *bytes*); este código é depois anexado à trama antes de se iniciar a cifra dos dados. Como o MIC é uma função dos endereços MAC de origem e destino, a trama fica associada ao emissor e ao receptor, eliminando-se assim a possibilidade de ataques por falsificação.

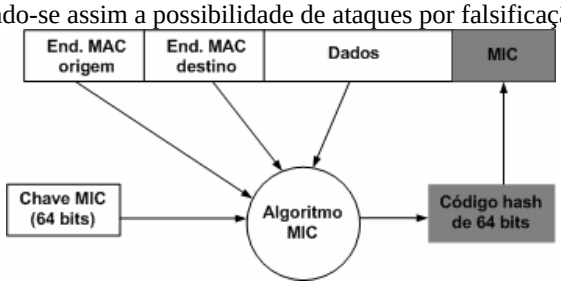



Figura 1. Determinação do MIC.

O receptor de uma trama cifrada determina o MIC. Se o resultado for igual ao MIC enviado, então garante-se que a mensagem é autêntica; caso contrário a mensagem é falsa. Caso ocorram duas falsificações de mensagem no mesmo segundo, as chaves devem ser apagadas e o cliente deve desassociar-se do AP e voltar a realizar o processo de autenticação.

*A.2. IV estendido/ Novo contador de sequência de IV*

A utilização de IV estendidos elimina o problema de re-utilização de IV, tornando mais difícil para um atacante descobrir a chave de cifra. As regras de sequenciação dos IVs eliminam o perigo de ataques de repetição: sempre que uma mensagem contiver um IV com um número de sequenciação de uma mensagem mais antiga é eliminada.

O TKIP utiliza um IV de 48 *bits*, enquanto que o WEP utiliza um IV de apenas 24 *bits*: este aumento do tamanho do IV permite aumentar a probabilidade de obter pares chave-IV únicos. O novo IV do TKIP é obtido com o primeiro e o último *byte* do IV WEP e um novo IV de quatro *bytes* (Figura 2). A trama que se obtém utilizando o TKIP é doze *bytes* maior que a trama WEP (4 *bytes* para o IV estendido e 8 *bytes* para o MIC), o que representa um aumento no *overhead* introduzido.

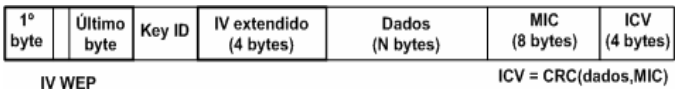



Figura 2. Trama TKIP.

Os dois *bytes* obtidos do IV do WEP são combinados de modo a serem utilizados como contador de sequência. Este contador é denominado TKIP *Sequence Counter* (TSC) e é ele que permite prevenir contra ataques de repetição. A utilização do TSC é definida por um conjunto de regras: (1) inicia-se a sequência a zero sempre que se estabelecerem novas chaves; (2) o TSC é aumentado de um em cada pacote; (3) a transferência de informação termina se o TSC atingir o seu valor máximo; e (4) o receptor rejeita qualquer pacote recebido fora da sequência (esta característica é importante, já que pode indicar incompatibilidades entre o TKIP e o 802.11e).

*A.3. Geração de chaves por pacote/Gestão de chaves*

O objectivo da geração de chaves por pacote é eliminar a utilização de chaves fracas. Esta chave é obtida pela combinação do endereço do emisssor, do IV de 48 *bits* e de uma chave de 128 *bits* denominada de chave temporal. O nome *chave temporal* advém do facto de que essa chave é alterada assim que é re-iniciada a contagem de sequência. A chave por pacote é então utilizada para cifrar os dados, o MIC e o ICV.

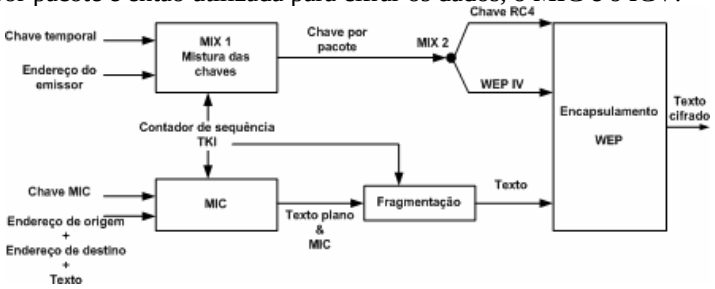



Figura 3. TKIP: computação do MIC e geração de chaves por pacote.

A obtenção da chave temporal é o resultado de um processo hierárquico de gestão de chaves. O protocolo de autenticação da camada de rede permite obter uma chave de sessão denominada *Master Key* (MK); essa chave é depois utilizada para obter a *Pairwaise Master Key* (PMK), que por sua vez é utilizada para se obter a chave temporal, designada por *Pairwaise Transient Key* (PTK), que será utilizada para cifrar os dados.

O processo de geração de chave por pacote encontra-se ilustrado na Figura 3. A chave temporal não é directamente utilizada para cifrar os dados: esta passa por um processo que elimina os padrões que podem ser usados para se realizarem ataques às chaves fracas. A fase 1 da função de mistura (MIX 1) é utilizada para eliminar a possibilidade de utilização da mesma chave em todas as ligações; a fase 2 da função de mistura (MIX 2) é utilizada para eliminar a relação entra a chave temporal e o IV [13].

*B. Protocolo de autenticação 802.1X*

Um dos maiores defeitos do WEP é o facto de a identidade de um cliente nunca ser na realidade validada através de qualquer tipo de integridade. O WPA elimina este defeito utilizando autenticação na camada superior, ou seja, na camada de rede. O protocolo utilizado para implementar essa autenticação é o 802.1X [1]. A *Wi-Fi Alliance* recomenda para autenticação na camada de rede a implementação 802.1X baseada no protocolo de autenticação *Extensible Authentication Protocol – Transport Layer Security* (EAP-TLS) [8]. Uma autenticação EAP-TLS bem sucedida tem como resultado a determinação de uma chave de sessão que será depois utilizada, tal como referido na secção anterior, para dar origem à chave temporal que permitirá cifrar os dados.

Para ser possível a utilização do mecanismo de autenticação 802.1X é necessário utilizar um servidor de autenticação. O servidor de autenticação que normalmente se utiliza é um servidor *Remote Access Dial-In User Service* (RADIUS) [5]. Assim sendo, será responsabilidade do servidor RADIUS autenticar (ou não) de forma bem sucedida um cliente da rede sem fios, e será também sua responsabilidade a determinação da chave de sessão (chave RADIUS). É importante referir que, dadas as características do 802.1X, apenas é utilizado o protocolo RADIUS para comunicação entre o AP e o servidor de autenticação. Na rede sem fios, entre o cliente e o AP, é utilizado o protocolo EAP.

Os três elementos principais do processo de autenticação 802.1X/EAP são a autenticação mútua entre o cliente e o servidor de autenticação (RADIUS), as chaves de codificação/cifra derivadas dinamicamente após a autenticação, e a política de controlo centralizado, que inclui a activação de mecanismos de re-autenticação no fim de sessão e geração de novas chaves. Quando estas características estão implementadas, um cliente que se associa a um AP, enquanto não efectuar um *login* na rede, não obtém acesso aos recursos da mesma. Depois de associado, o cliente e a rede (AP ou servidor RADIUS) trocam mensagens EAP de forma a realizarem autenticação mútua; o cliente verifica as credenciais do servidor RADIUS e vice-versa.

*C. Funcionamento geral do WPA-EAP*

O funcionamento do WPA é caracterizado por quatro fases (Figura 4): a fase da descoberta das capacidades de segurança entre o AP e o cliente, a fase de autenticação 802.1X entre o cliente e o servidor de autenticação, a fase da distribuição de chaves RADIUS do servidor de autenticação para o autenticador, e a fase de gestão das chaves 802.1X entre o autenticador e o cliente.

A fase da descoberta das capacidades de segurança tem como objectivo determinar possíveis pares com quem estabelecer comunicações e anunciar as capacidades de segurança da rede aos clientes. Nesta fase, o cliente envia um pedido de associação ao AP; o AP bloqueia todos os pedidos de acesso à rede, e apenas permite o envio de mensagens 802.1X. Nesta fase, o AP indica ao cliente que protocolo de cifra é utilizado para proteger as comunicações.

A fase de autenticação 802.1X tem como objectivo tornar o servidor num centro de decisão das políticas de acesso à rede e efectuar autenticação mútua entre o cliente e o servidor. Para ser possível a autenticação mútua, o cliente e o servidor trocam mensagens 802.1X. Nestas mensagens é enviada toda a informação relativa às credenciais de autenticação do servidor de autenticação e do cliente. Nesta fase são também geradas a MK e a PMK.

A fase da distribuição de chaves tem como objectivo o envio da chave PMK do servidor de autenticação ao AP.

Finalmente, a fase da gestão de chaves tem como objectivos: associar a PMK ao AP e ao cliente, permitir que tanto o AP como o cliente confirmem que conhecem a PMK (autenticação mútua entre o AP e o cliente), gerar e sincronizar a utilização da chave PTK (processo conhecido por *four-way handshake*), e efectuar a distribuição da chave de cifra *broadcast* GTK (*Group Transient Key*).

Após estes processos, o AP e o cliente podem comunicar de forma segura.

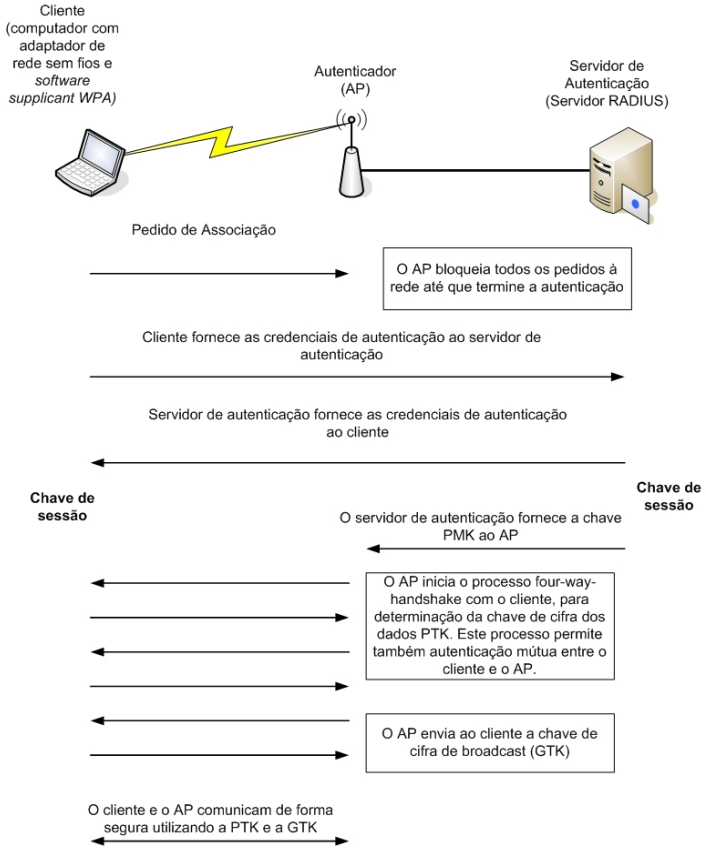



Figura 4. Funcionamento do WPA-EAP.

*D. WPA-PSK*

A *Wi-Fi Alliance* definiu um outro modo de funcionamento do WPA denominado de WPA-*Pre Shared Key* (PSK), para situações em que não é possível a utilização de uma infra-estrutura de autenticação. Neste modo de funcionamento, a chave PMK deve ser previamente configurada no AP e no cliente. A **Figura 5** apresenta a implementação de um sistema WPA-PSK. Como ilustrado na figura, para a implementação WPA-PSK é apenas necessário um AP com suporte WPA e clientes da rede sem fios com o *software* cliente WPA (*supplicant* WPA). Como neste modelo de operação não é efectuada a autenticação dos utilizadores, é apenas necessário efectuar o processo *four-way-handsha*ke para obtenção da chave PTK. Depois de obtida a PTK é calculada a chave GTK da mesma forma que para o sistema WPA.


Figura 5. Sistema WPA-PSK.

Este modo de funcionamento introduz a possibilidade de um intruso efectuar ataques de dicionário à PMK configurada no cliente, permitindo-lhe aceder à rede de forma não autorizada. As principais vantagens deste sistema são a simplicidade de implementação e de configuração, não sendo necessário implementar um servidor de autenticação.

## III. Experimentação e Resultados

Para ser possível avaliar as capacidades de segurança e o custo ao nível do desempenho da rede e dos equipamentos implementou-se em laboratório, recorrendo-se a ferramentas em código aberto, uma rede protegida pelo WPA, nas suas variantes WPA-EAP (Figura 6) e WPA-PSK. Utilizou-se como sistema operativo em todas as implementações o *Linux*, na sua distribuição *Mandrake* 9.2. A versão do servidor *FreeRADIUS* utilizado foi a 1.01; para o *software OpenSSL* utilizou-se a versão 0.9.7d. Como cliente WPA, utilizou-se a versão 0.2.7 do software *wpa_supplicant.* Em todas as implementações utilizou-se *hardware* 802.11g, o que permitiu recriar um ambiente totalmente 802.11g. O método de autenticação EAP utilizado é o TLS. Este método utiliza certificados digitais para autenticação dos utilizadores e do servidor de autenticação (servidor RADIUS), o que garante a protecção contra ataques do *homem no meio*, personificação e controlo de sessão. A principal desvantagem deste método é o seu nível de complexidade para sistemas com um número elevado de utilizadores.

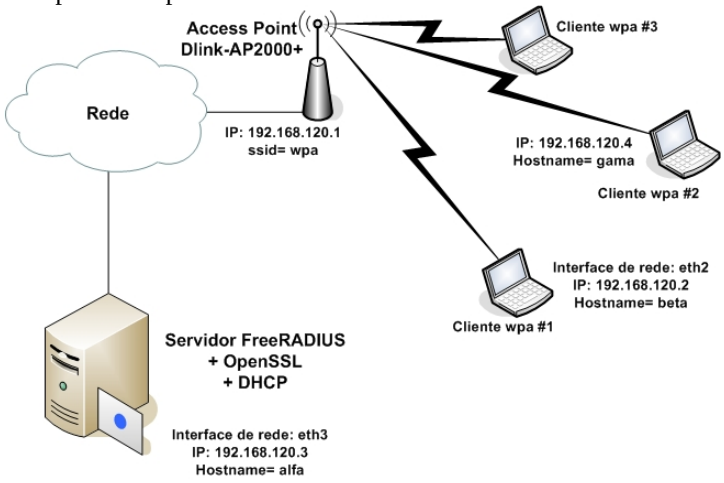



Figura 6. Cenário experimental WPA-EAP.

Esta secção tem três objectivos distintos. O primeiro consiste em verificar experimentalmente o funcionamento das soluções WPA, tendo em conta as mensagens que são trocadas entre os diversos elementos nos processos de negociação de chaves, autenticação e envio de informação protegida. O segundo objectivo consiste em averiguar a eficiência das soluções WPA ao nível da sua resistência a ataques de segurança. Finalmente, pretende-se averiguar o desempenho e complexidade das soluções ao nível do *throughput*, atrasos na rede, variação do atraso (*jitter*) e a carga de processamento nos equipamentos. Os resultados das experiências de desempenho da rede são comparados entre si, e também com os resultados de uma rede a funcionar sem o recurso a qualquer implementação de segurança (rede plana), para ser possível determinar o verdadeiro custo que cada implementação introduz na rede.

Esta secção é organizada da seguinte forma: na sub-secção *A* apresenta-se uma análise ao funcionamento do WPA; a sub-secção *B* descreve os ataques à segurança dos protocolos implementados e os resultados por eles obtidos; a sub-secção *C* apresenta os testes e resultados de desempenho da rede das soluções implementadas e os resultados de complexidade computacional.

### *A. Funcionamento do WPA*

A análise do funcionamento da negociação WPA-EAP é dividida em duas partes, uma que corresponde à troca de mensagens entre o cliente WPA e o AP, onde as mensagens são enviadas utilizando o protocolo EAP, e outra correspondente à troca de mensagens entre o AP e o servidor RADIUS, sendo o protocolo RADIUS o responsável

pelas trocas de mensagens. A Figura 7 representa toda a troca de mensagens entre o AP e o cliente (pacotes 1 a 20). A Figura 8 em contrapartida representa as mensagens necessárias à negociação entre o AP e o servidor (pacotes 2 a 17). Convém referir que apenas o cliente e o servidor suportam a autenticação EAP-TLS; o AP apenas suporta o processo de autenticação 802.1X/EAP.

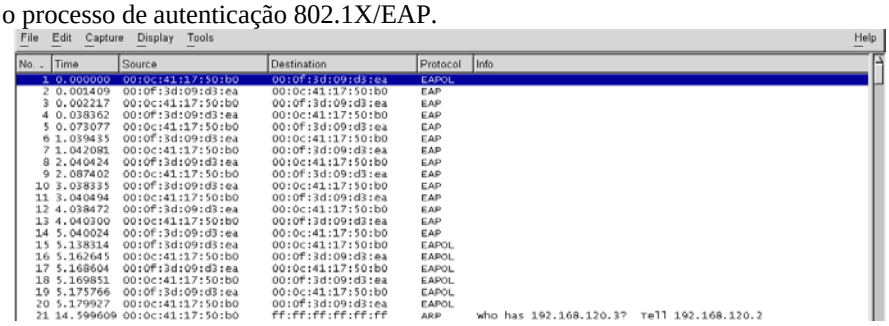



Figura 7. Mensagens WPA-EAP do cliente.

O processo de negociação do protocolo WPA-EAP é dividido em duas partes. Numa primeira parte (que corresponde às fases da descoberta das capacidades de segurança entre o AP e o cliente, a fase de autenticação 802.1X entre o cliente e o servidor de autenticação e a fase da distribuição de chaves RADIUS do servidor de autenticação para o autenticador) é efectuada a autenticação mútua entre o cliente e o servidor de autenticação (autenticação TLS). Esta parte está representada pelos pacotes 1 a 14 da Figura 7 e pelos pacotes 2 a 17 da Figura 8. Nesta parte o AP apenas encaminha as mensagens entre o cliente e o servidor, e efectua também o encapsulamento das mensagens EAP em mensagens RADIUS e vice-versa. Na segunda parte do processo (fase de gestão das chaves 802.1X entre o autenticador e o cliente) são derivadas as chaves utilizadas para proteger a comunicação entre o cliente e o AP. Esta parte está definida pelos pacotes 15 a 20 da **Figura 7**. Esta parte utiliza apenas comunicação entre o cliente e o AP. A negociação das duas partes do protocolo WPA-EAP tem uma duração aproximada de 5 segundos.

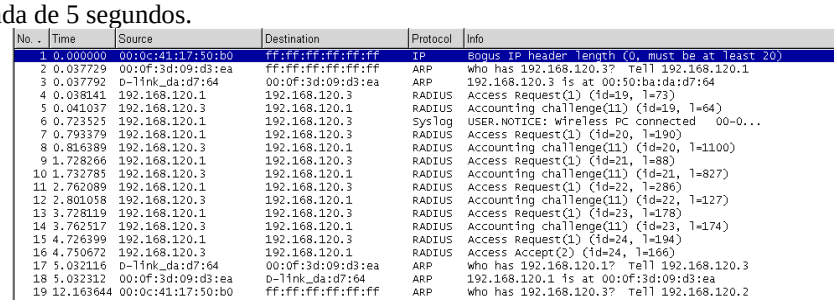



Figura 8. Mensagens WPA-EAP do servidor.

O resultado da análise ao funcionamento da negociação WPA-PSK está apresentado na Figura 9. A principal diferença entre o funcionamento do WPA-PSK e do WPA-EAP é que o primeiro não inclui a fase de autenticação de nível de rede. A autenticação é baseada numa palavra-chave partilhada pelo AP e pelo cliente, sendo apenas efectuado o processo conhecido como *four-way handshake* para determinação das chaves utilizadas para cifrar os dados das comunicações. A negociação do protocolo WPA-PSK tem uma duração aproximada de 0.2 segundos - a primeira trama corresponde a uma autenticação falhada (falta de resposta do AP - *timeout*), não sendo por isso contabilizada.

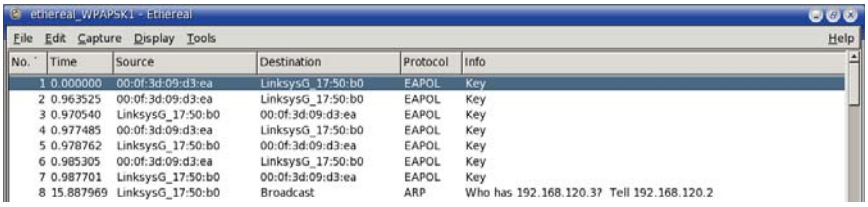



Figura 9. Mensagens WPA-PSK.

A análise ao funcionamento das variantes WPA-EAP e WPA-PSK permite verificar que o funcionamento da variante WPA-PSK é muito mais simples, já que apenas são necessários dois intervenientes. Ao nível do *overhead*, os valores apresentados pelo protocolo WPA-PSK são semelhantes ao do protocolo WPA-EAP, o que indica que as mensagens não sofrem grandes alterações, mantendo-se praticamente inalteradas. Devido ao facto de ser um sub-conjunto do WPA-EAP, a negociação do WPA-PSK é mais rápida.

*B. Reacção a Ataques de Segurança*

Para determinar as capacidades de segurança do WPA configura-se uma máquina cliente da rede sem fios a funcionar como intruso. Nesta máquina instala-se a ferramenta *ettercap* [11]. Esta ferramenta é considerada um

*canivete suíço* nos ataques às redes, pois permite realizar ataques de *homem no meio*, personificação, controlo de sessão e negação de serviço de uma forma muito simples. Os ataques de personificação, *homem no meio* e controlo de sessão realizados ao WPA-EAP falharam; o ataque de negação de serviço foi realizado com sucesso.
Para realizar o ataque de personificação configura-se o intruso com o mesmo endereço IP, mesmo *hostname* e com certificados digitais com o mesma designação que o cliente autorizado, não sendo possível ao intruso efectuar a autenticação na rede. Quando o servidor solicitava o certificado do cliente este não era reconhecido como cliente autorizado.
Para a realização do ataque *homem no meio* utiliza-se, para tentar obter a informação que circulava na rede WPA, a ferramenta *ettercap*. Como o *ettercap* funciona ao nível da camada de rede e o WPA é um protocolo da camada de ligação de dados não foi possível efectuar o ataque.
Para se efectuar o ataque de controlo de sessão tenta-se, novamente com o *ettercap*, injectar e alterar mensagens que circulavam na rede. O intruso não obteve resposta de nenhum dos intervenientes no sistema, já que o AP elimina essas mensagens devido ao mecanismo TSC, falhando assim o ataque.
Para a realização do ataque de negação de serviço utiliza-se um *software* cliente WPA no intruso. Assim, tenta-se de forma continuada efectuar o pedido de autenticação na rede. Estes pedidos bloquearam o AP, não permitindo que mais nenhum cliente autorizado se autenticasse no sistema e tivesse acesso aos recursos da mesma.
Ao WPA-PSK foi possível efectuar ataques passivos de dicionário. Para a realização destes ataques de segurança utilizam-se ferramentas como o *coWPAtty* [9] e *ptcrack* [10] que permitem, mediante a sua utilização, determinar a palavra-chave partilhada entre o AP e o cliente em aproximadamente cinco minutos. A utilização destas ferramentas é muito simples e divide-se em duas fases. Numa primeira fase é necessário recolher as mensagens do processo *four-way handshake* (ferramenta *ethereal*); na segunda fase utiliza-se uma das ferramentas para se obter a chave PMK.
Para efectuar este tipo de ataque com a ferramenta *coWPAtty*, utiliza-se a ferramenta *ethereal* para se obter um registo das mensagens da negociação do processo *four-way handshake* (ficheiro *eap-psk.dump*) do WPA-PSK.
Como exemplo, apresentam-se alguns detalhes do processo de realização deste ataque e os resultados obtidos. A ferramenta *coWPAtty* é activada da seguinte forma:

*# ./cowpatty -r eap-psk.dump -f dict -s wpa*

Cerca de 5 minutos após a activação da ferramenta surge a mensagem:

*The PSK is "thewindinthewillows".*

Deste modo obtém-se a PMK. Assim, é possível configurar qualquer cliente com essa PMK e aceder à rede protegida pelo WPA-PSK. Os ataques possíveis de ser efectuados com a utilização da PMK são ataques aos serviços de integridade, confidencialidade, autenticação e não-repúdio. Depois de concluída a configuração do intruso com a PMK, o intruso autentica-se na rede. Convém referir, no entanto, que a chave PMK utilizada é uma chave fraca, sendo muito fácil de obter recorrendo a ataques de dicionário. Para tornar a chave mais forte, esta deveria ter mais caracteres (superior a 25 caracteres) e utilizar caracteres pouco comuns como o ?, %, $, #,etc. De seguida, utiliza-se a ferramenta *ethereal*, tentando obter a informação trocada entre um cliente válido e a rede. A Figura 10 ilustra a captura de um intruso obtida com a ferramenta *ethereal*. O intruso consegue obter o nome de utilizador (*USER*) e a palavra-chave (*PASS*) de um cliente quando este tenta estabelecer uma sessão com um servidor FTP.
Pode-se concluir que a solução WPA-EAP é mais resistente a ataques de segurança que a solução WPA-PSK. É possível, e de forma muito simples, realizar ataques de dicionário ao WPA-PSK, e assim ter acesso a todos os recursos da rede.

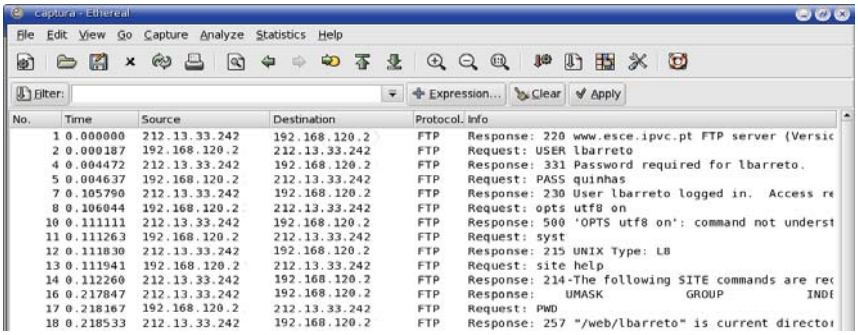


Figura 10. Captura *ethereal* depois de obtida a PMK.

*C. Desempenho da Rede e dos seus Equipamentos*

Os testes de desempenho dividem-se em duas partes: numa primeira parte efectuam-se testes que permitem avaliar o desempenho da rede; numa segunda parte efectuam-se testes de desempenho aos equipamentos (servidores e clientes). Para a realização dos testes de desempenho da rede utiliza-se a ferramenta *IPERF* [14]. As ferramentas utilizadas para avaliar o desempenho dos equipamentos são o *sysstat* [15] e o comando do *Linux vmstat*.
Para melhor se avaliar o custo acrescido no desempenho da rede pela introdução dos protocolos de segurança implementados, realizam-se também testes de desempenho da rede numa situação em que esta se encontra sem mecanismos de segurança (rede plana). A **Figura 11** indica quais os equipamentos utilizados para os testes de desempenho *IPERF*, bem como a localização do cliente e servidor *IPERF*. Os resultados apresentados representam o valor médio obtido pela realização de 8 experiências.

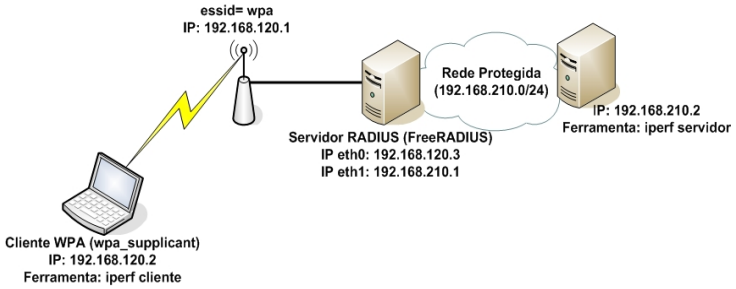



Figura 11. Utilização IPERF implementação WPA-EAP.

Os primeiros testes de avaliação do desempenho da rede consistem na determinação do *throughput* (quantidade de informação enviada, em *bytes*, num determinado intervalo de tempo). O primeiro fluxo de tráfego TCP gerado tem uma janela de 85.3 *Kbytes* (este valor é definido por defeito pelo *IPERF*), o que significa que por cada 85.3 *Kbytes* enviados, o receptor deve confirmar a recepção dos mesmos. Todos os fluxos aqui utilizados têm uma duração de 20 segundos. O fluxo é gerado após a negociação do WPA ter concluído com êxito.
O gráfico da Figura 12 mostra o resultado obtido pelo *IPERF* para esse fluxo de tráfego. Os resultados presentes no gráfico permitem concluir que as implementações WPA apresentam um desempenho próximo do sistema plano. Estas similaridades dos resultados devem-se ao facto de as implementações WPA apenas cifrarem com uma determinada chave de cifra o pacote IP e acrescentarem-lhe um IV, não alterando assim significativamente o tamanho nem o formato do mesmo. Além disso, a utilização do algoritmo de cifra o RC4 é de processamento fácil, não alterando por isso o desempenho da rede.
O melhor desempenho da implementação WPA-EAP em relação à WPA-PSK pode estar relacionado com a forma de funcionamento do protocolo TCP. Sempre que ocorrer uma perda de pacotes, o TCP interpreta esta indicação como congestionamento da rede e diminui a taxa de transmissão da informação. As perdas de pacotes podem ser originadas pela falta de capacidade do *buffer* do AP em armazenar todos os pacotes recebidos, pela impossibilidade deste processar todos os pacotes e pelo maior número de pacotes a circular na rede. Como os resultados das implementações WPA são obtidos para janelas TCP e pacotes de igual tamanho, e como todo o processo de protecção de dados (cifra e decifra) nas duas implementações é exactamente igual, o melhor desempenho da implementação WPA-EAP poderá ser consequência, para aquele momento, das condições da rede.

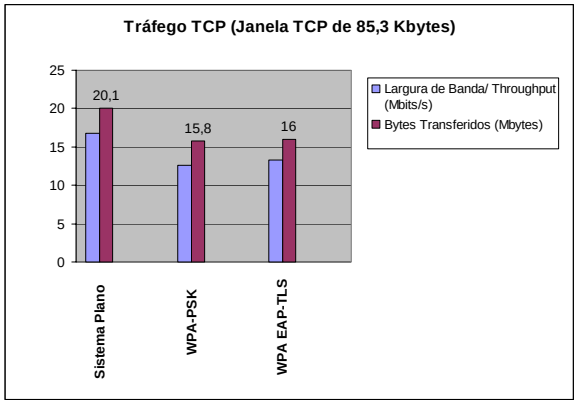



Figura 12. *Troughput* e informação enviada – fluxo TCP de 85,3 *Kbytes*.

Para simular a utilização da rede por aplicações diferentes definem-se tamanhos de mensagens com valores compreendidos entre 8 e 4096 *bytes*. Os resultados obtidos encontram-se apresentados na Figura 13. Verifica-se que, para os diversos valores de tamanho das mensagens, a implementação WPA apresenta um comportamento semelhante ao do sistema plano. Também se pode verificar que o seu desempenho é melhor para mensagens de tamanho superior a 2000 *bytes*. Este resultado está relacionado com o facto de, sendo o tamanho da janela TCP

um valor fixo, quanto maior o tamanho das mensagens, menor o número de mensagens a enviar para a mesma janela TCP, o que reduz o número de colisões, aumentando o desempenho da rede.

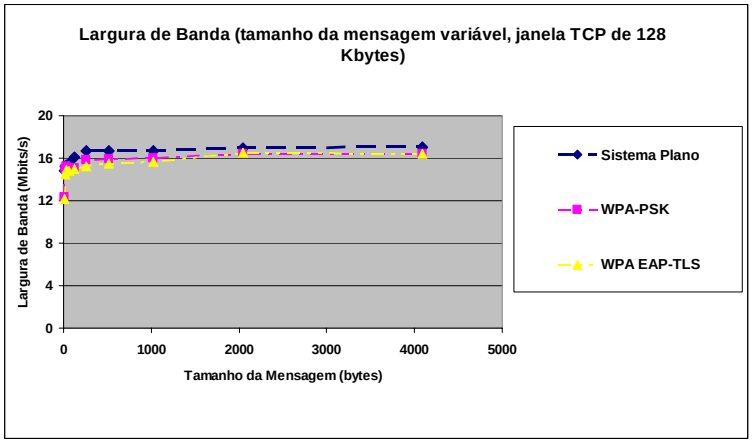
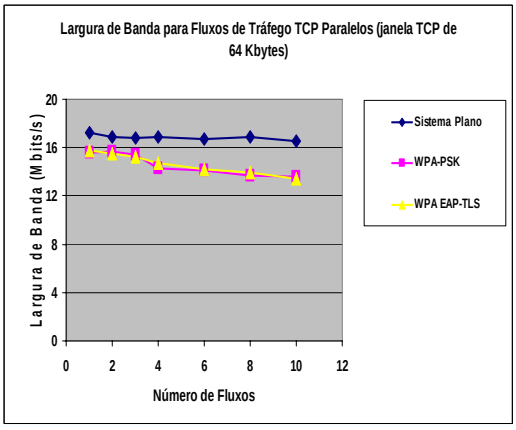
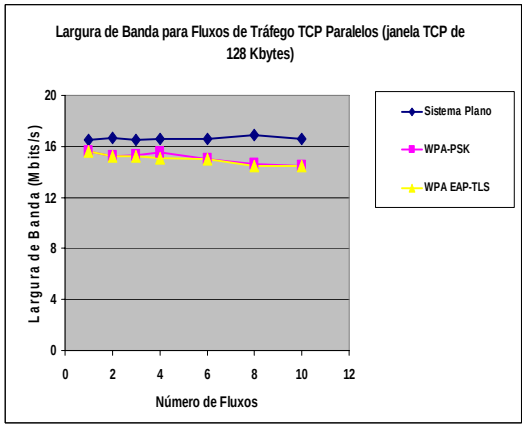



Figura 13. *Throughput* para mensagens de tamanho variável.

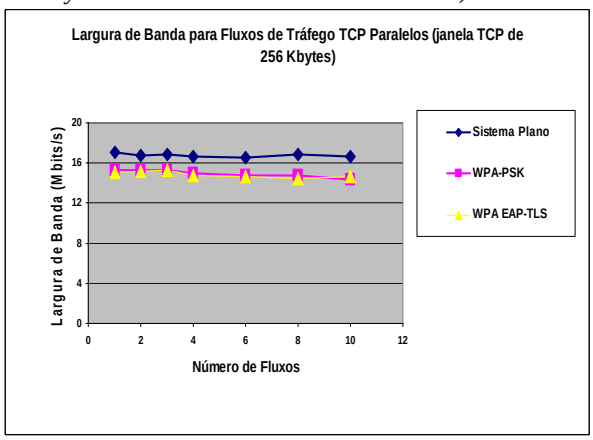
Para simular a utilização da rede por vários clientes em simultâneo e a utilização de diversas aplicações, utilizaram-se fluxos de tráfego TCP com janelas de 64, 128 e 256 *kbytes*, com 1 a 10 fluxos de tráfego em simultâneo. Esta experiência tem a duração de 10 segundos para cada fluxo. A **Figura 14** apresenta os resultados obtidos. Uma análise das figuras permite concluir que, à medida que o número de clientes aumenta, o desempenho dos sistemas WPA diminui de forma significativa. O aumento do número de clientes implica o aumento do número de mensagens a circular na rede, e consequentemente o aumento do número de colisões (e diminuição da taxa de transmissão). Outro factor que contribui para a diminuição da taxa de transmissão é o aumento do número de mensagens recebidas pelo AP quando o número de clientes aumenta. Como o AP não tem capacidade para processar todas as mensagens recebidas, rejeita um maior número de mensagens, o que leva o TCP a activar o mecanismo de controlo de congestionamento da rede.




a) Janela TCP de 64 *Kbytes.*



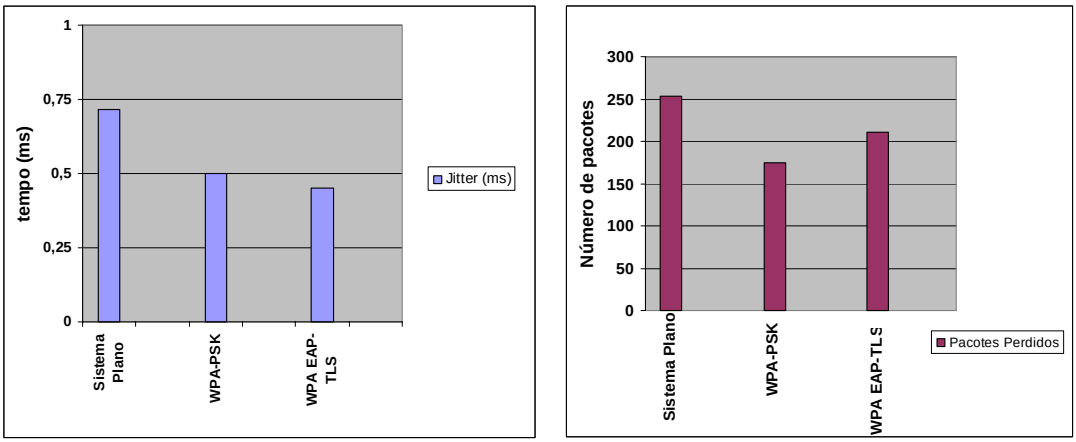

b) Janela TCP de 128 *Kbytes*




c) Janela TCP de 256 *Kbytes*

Figura 14. *Throughput* para fluxo de tráfego TCP.

De seguida apresenta-se a variação do atraso (*jitter*) e o número de pacotes perdidos nas diferentes soluções. Para estas experiências são utilizados fluxos de dados UDP. As experiências realizadas utilizam um fluxo UDP com datagramas de 1500 *bytes*, *buffer* UDP de 64 *Kbytes* e largura de banda de 10 *Mbits/s*. A **Figura 15** apresenta os resultados. Nesta experiência são gerados 10 fluxos de dados UDP com a duração de 10 segundos. Pela observação dos gráficos verifica-se que a variação do atraso é um pouco superior para o sistema plano. Este resultado pode ser explicado pelo facto de o AP estar mais congestionado no sistema plano (maior envio de pacotes).

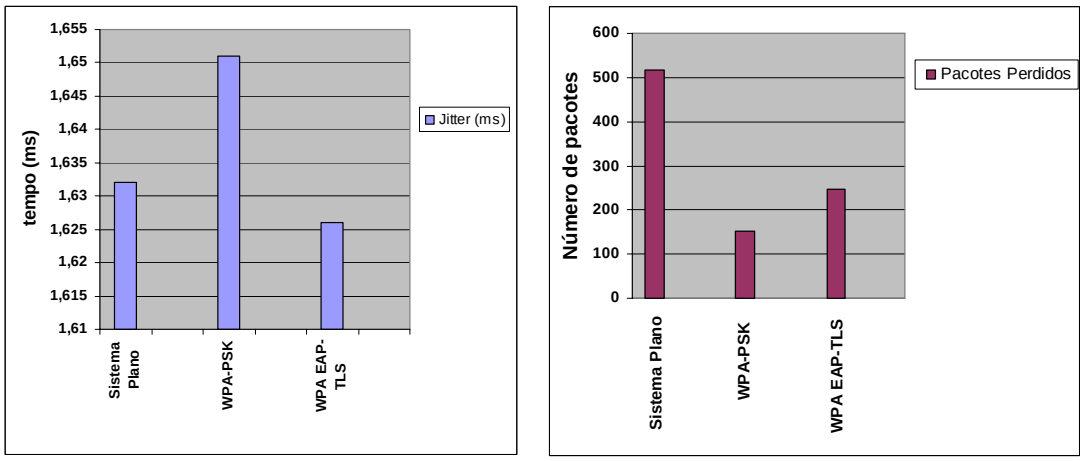



a) *Jitter* b) Pacotes perdidos.

Figura 15. *Jitter* e número de pacotes perdidos – largura de banda=10*Mbits/s*.

Em relação ao número de pacotes perdidos, as implementações WPA apresentam também melhores resultados que a rede plana. Estes resultados estão também relacionados com o facto de o sistema plano não efectuar qualquer alteração dos pacotes, conseguindo no mesmo espaço de tempo gerar maior número de pacotes que os sistemas WPA, o que poderá aumentar as colisões de pacotes e, consequentemente, o número de pacotes perdidos. O maior número de pacotes perdidos do sistema WPA-EAP, relativamente ao sistema WPA-PSK, poderá estar relacionado com a condição da rede no momento da realização dos testes.

A Figura 16 apresenta os valores da mesma experiência, mas para uma largura de banda disponível de 54 *Mbits/s* (802.11*g*). Os resultados obtidos reforçam os valores anteriormente obtidos para a largura de banda de 10 *Mbits/s*.

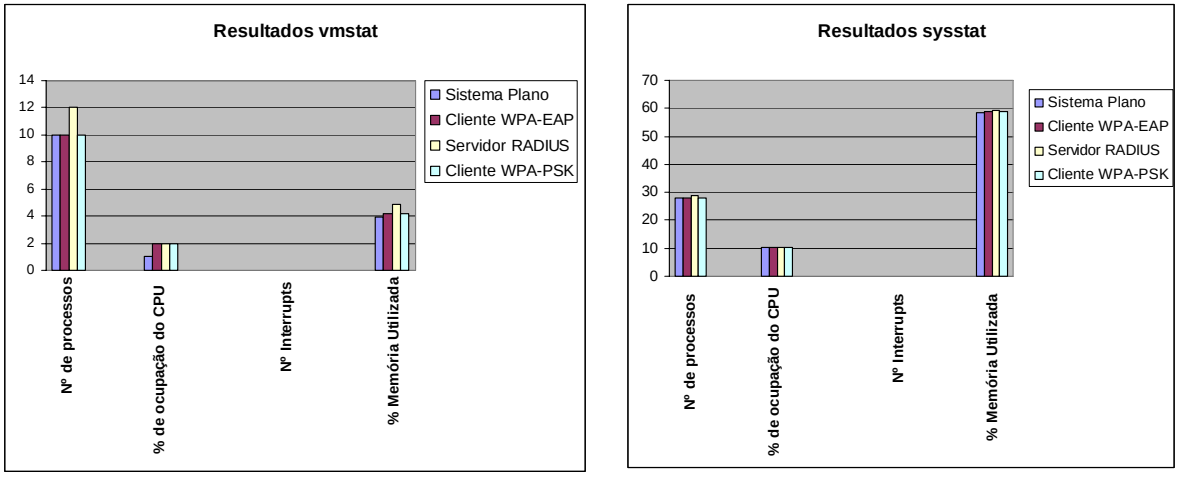



a) *Jitter*. b) Pacotes perdidos.

Figura 16. *Jitter* e número de pacotes perdidos – largura de banda=54*Mbits/s*.

As experiências de desempenho da rede realizadas permitem-nos concluir que a utilização do WPA não introduz custos significativos na rede.

Para avaliar o desempenho dos equipamentos, nomeadamente dos servidores e dos clientes da rede sem fios, utilizam-se como ferramentas o *sysstat* e o *vmstat* incluído no *Linux*. O *sysstat* é um conjunto de ferramentas que permite medir o desempenho de uma máquina *Linux*, ao nível do processamento, IO, memória e de actividade do sistema. O *vmstat* é um comando *Linux* que reporta estatísticas sobre *kernel threads*, memória, discos, actividade do processador e *traps*. Convém mencionar que a sua utilização acarreta custos consideráveis no sistema. Para se obterem os resultados foi necessário incluir as ferramentas no cliente WPA e no servidor de autenticação (servidor RADIUS).




a) Ferramenta *vmstat.* b) Ferramenta *sysstat.*

Figura 17. Desempenho dos equipamentos.

Os resultados observados na Figura 17 permitem verificar que a utilização do WPA não implica um aumento das necessidades do sistema, sendo os diferentes valores semelhantes. As principais diferenças de valores indicados por cada uma das ferramentas devem-se aos custos específicos introduzidos por cada uma das ferramentas. Estes estão directamente relacionados com a forma de implementação, de interacção com o sistema e de obtenção dos resultados das ferramentas. Pode-se concluir que a ferramenta *sysstat* é aquela que, no seu funcionamento, utiliza mais memória e também mais processos para obter os resultados. A ferramenta *vmstat* necessita de um maior número de *Interrupts* e de maior percentagem de ocupação do CPU.

## IV. CONCLUSÃO

Este artigo apresentou uma descrição dos componentes do WPA, um estudo das suas capacidades de segurança e o custo por ele introduzido no desempenho da rede e dos equipamentos.

Ao nível das capacidades de segurança do WPA foi possível verificar, para a solução EAP-TLS, a protecção deste sistema em redes sem fios contra ataques do tipo *homem no meio*, personificação e controlo de sessão. Relativamente a ataques de negação de serviço, o WPA não se mostrou muito eficaz, sendo possível efectuar este tipo de ataques sem grandes requisitos no sistema.

Relativamente ao desempenho da rede foi possível verificar que o mecanismo WPA não diminui de forma significativa o desempenho da mesma. Verificou-se também que o desempenho da rede de um sistema WPA diminui com o aumento do número de clientes presentes na rede devido ao aumento das necessidades dos APs. Os testes ao desempenho dos equipamentos permitem concluir que a introdução do mecanismo WPA não afecta o seu desempenho, mantendo-se os valores praticamente inalterados para soluções WPA e rede plana.

## REFERÊNCIAS


[1] IEEE Std. 802.11b (1999), Supplement to ANSI/IEEE Std. 802.11, 1999 Edition, Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band. 1999.http://standards.ieee.org/getieee802/

[2] Página da *Wi-Fi Alliance*, http://www.wi-fi.org

[3] Página do WPA, http://www.wi-fi.org/OpenSection/protected_access_archive.asp

[4] IEEE Std. 802.11i (2004), Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)Specifications Amendment 6: Medium Access Control (MAC) security Enhancements.2004.http://standards.ieee.org/getieee802

[5] Carl Rigney, A.C.R., William Allen Simpson, Steve Willens, *Remote Authentication Dial In User Service (RADIUS)*, *RFC2138*. 1997.

[6] Página da RSA, http://www.rsasecurity.com

[7] IEEE Std. 802.1x (2001), *Port-Based Network Access Control*, 2001. http://standards.ieee.org/getieee802/

[8] B. Aboba, D.S., *PPP EAP TLS Authentication Protocol, RFC2716*. 1999.

[9] Página da implementação *coWPAtty*, http://sourceforge.net/projects/cowpatty

[10] Página da implementação *Ptcrack*, http://sourceforge.net/projects/ptcrack

[11] Página da ferramenta de realização de ataques MITM *Ettercap*, http://ettercap.sourceforge.net/

[12] Página do analisador de protocolos *Ethereal*, http://www.ethereal.com

[13] Jesse Walker, *802.11 Security Séries Part II: The Temporal Key Integrity Protocol*. 2002.http://cedar.intel.com/media/pdf/security/80211_part2.pdf

[14] Página da implementação *IPERF*, http://dast.nlanr.net/Projects/Iperf/
[15] Página da implementação *Sysstat*, http://perso.wanadoo.fr/sebastien.godard